PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Ito et al.

Group No.:

Express Mail: EF297166669US

Examiner:

Filed: January 3, 2001

For: CONTROL PROGRAM, DEVICE INCLUDING THE CONTROL PROGRAM, METHOD FOR CREATING THE CONTROL PROGRAM, AND METHOD FOR OPERATING THE CONTROL PROGRAM

Assistant Commissioner for Patents
Washington, D.C. 20231

TRANSMITTAL OF CERTIFIED COPY

Attached please find the certified copy of the foreign application from which priority is claimed for this case:

Country: Japan
Application Number: 2000-005501
Filing Date: January 14, 2000

SIGNATURE OF ATTORNEY

Reg. No. 26,725 Neil A. DuChez

Tel. No. (216) 621-1113 **RENNER, OTTO, BOISSELLE & SKLAR, P.L.L.**
1621 Euclid Avenue
Nineteenth Floor
Cleveland, Ohio 44115

(Translation)

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application : January 14, 2000

Application Number : Patent Appln. No. 2000-005501

Applicant(s) : MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.

Wafer of the Patent Office

December 8, 2000

Kozo OIKAWA

Commissioner,
Patent Office

Seal of Commissioner of the Patent Office

Appln. Cert. No. Appln. Cert. Pat. 2000-3103202

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　１月１４日

出願番号
Application Number: 特願２０００－００５５０１

出願人
Applicant (s): 松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１２月　８日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３１０３２０２

【書類名】　特許願

【整理番号】　2032410442

【提出日】　平成12年 1月14日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

G11B 20/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　伊藤　基志

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　植田　宏

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　佐々木　真司

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　制御プログラム隠蔽方法および制御プログラムが隠蔽された装置

【特許請求の範囲】

【請求項１】　データを変換するデータ変換回路を備えた装置の制御プログラム隠蔽方法であって、

制御プログラムの一部に前記データ変換回路の逆変換を施すプログラム逆変換ステップと、

前記プログラム逆変換ステップにより一部が逆変換された制御プログラムをプログラムメモリに格納するプログラム格納ステップと、

を包含することを特徴とする制御プログラム隠蔽方法。

【請求項２】　データを変換するデータ変換回路を備えた装置の制御プログラム隠蔽方法であって、

制御プログラムの一部である対象プログラムをプログラムメモリから書換可能メモリにコピーするプログラム複製ステップと、

前記プログラム複製ステップによりコピーされた対象プログラムを前記データ変換回路によって変換するプログラム変換ステップと、

前記プログラム変換ステップにより変換された対象プログラムを実行するプログラム実行ステップと

を包含することを特徴とする制御プログラム隠蔽方法。

【請求項３】　前記制御プログラム隠蔽方法は、前記プログラム変換ステップにより変換された対象プログラムの実行が終了した後に、前記対象プログラムを書換可能メモリから消去するプログラム消去ステップをさらに包含する、請求項２に記載の制御プログラム隠蔽方法。

【請求項４】　請求項２または請求項３に記載の制御プログラムを備えた装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、装置組込み型の制御プログラムを隠蔽する方法および制御プログラムが隠蔽された装置に関するものである。

【０００２】

【従来の技術】

近年、音楽や映像といったコンテンツがディジタル化される中で、著作権を保護する重要度が増している。そこで、コンテンツを暗号化する手法が用いられている。この暗号化されたコンテンツを再生するには、暗号を解読する必要がある。そこで、再生装置を開発するために、ライセンスを結んで、暗号の解読方法を入手するのであるが、同時に解読方法が外に漏れないように、何らかの保護手段を講じて装置に組み入れることが求められる。

【０００３】

解読方法がＬＳＩなどのハードウェアに組み込まれている場合、ＬＳＩの製造技術をもつ専門の人でないかぎり、ＬＳＩの中のアルゴリズムを解析することは不可能である。しかしながら、暗号方式がソフトウェアによって組み込まれている場合、そのソフトウェアの実行ファイルから逆アセンブルなどで解析できる人、いわゆるハッカーと呼ばれる人達がいる。そうしたハッカーに対抗すべく、解析され難いソフトウェア（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｔ　Ｐｒｏｇｒａｍ）の技術がある。

【０００４】

【発明が解決しようとする課題】

しかしながら、ＬＳＩなどのハードウェアによる解読方法の組込みは、近年の開発競争においては、開発速度面とコスト面で不利に働く傾向がある。また、ソフトウェア技術だけによる保護は、ソフトウェア技術で解析が不可能とは言えない。

【０００５】

本発明は上記問題点に鑑み、装置組込み型の制御プログラムの特徴を生かした、ハードウェアとソフトウェアを組み合わせたプログラムの隠蔽方法を提供する。

【０００６】

【課題を解決するための手段】

本発明の制御プログラム隠蔽方法は、データを変換するデータ変換回路を備えた装置の制御プログラム隠蔽方法であって、制御プログラムの一部に前記データ変換回路の逆変換を施すプログラム逆変換ステップと、前記プログラム逆変換ステップにより一部が逆変換された制御プログラムをプログラムメモリに格納するプログラム格納ステップとを包んでおり、これにより上記目的が達成される。

【０００７】

本発明の制御プログラム隠蔽方法は、データを変換するデータ変換回路を備えた装置の制御プログラム隠蔽方法であって、制御プログラムの一部である対象プログラムをプログラムメモリから書換可能メモリにコピーするプログラム複製ステップと、前記プログラム複製ステップによりコピーされた対象プログラムを前記データ変換回路によって変換するプログラム変換ステップと、前記プログラム変換ステップにより変換された対象プログラムを実行するプログラム実行ステップとを包んでおり、これにより上記目的が達成される。

【０００８】

前記制御プログラム隠蔽方法は、さらに、前記プログラム変換ステップにより変換された対象プログラムの実行が終了した後に、前記対象プログラムを書換可能メモリから消去するプログラム消去ステップを包んでおり、これにより上記目的が達成される。

【０００９】

【発明の実施の形態】

以下、図面を参照しながら本発明の実施の形態を説明する。

【００１０】

図１は、本発明の実施の形態における装置の構成の一例を示すブロック図である。図１で示される装置１は、不揮発性メモリであるプログラムメモリ４と、プログラムメモリ４に格納された制御プログラムに従って装置１を制御する小型演算素子（ＭＰＵ：Ｍｉｃｒｏ　Ｐｒｏｃｅｓｓｅｒ　Ｕｎｉｔ）であるマイコン２と、マイコン２の作業データ等を一時的に格納する書換可能メモリであるＤＲＡＭ５と、データを可逆的に変換するデータ変換回路３と、その他の回路６と、

それらを接続する内部バス７から構成される。ここで、不揮発性メモリとしては、再生専用メモリや１回書込可能メモリ（Ｏｎｅ　Ｔｉｍｅ　ＲＯＭ）やフラッシュメモリなどがある。書換可能メモリとしては、データの保持動作が不要なスタティックメモリ（Ｓｔａｔｉｃ　Ｍｅｍｏｒｙ）やデータの保持動作が必要なダイナミックメモリ（Ｄｙｎａｍｉｃ　Ｍｅｍｏｒｙ）などがある。その他の回路としては、例えば情報記憶装置の場合は、データ誤り訂正回路などがある。

【００１１】

図２は、データ変換回路３の一例を示す回路図である。図２において、四角が１ビットのフリップフロップで、丸が１ビットの排他的論理和であり、基本的にクロック１周期で左側に１ビットずつデータを移動するシフトレジスタのようなものである。これは、エラー訂正理論で用いられる８次の原始多項式（Ｐｒｉｍｉｔｉｖｅ　ｐｏｌｙｎｏｍｉａｌ）であるＰ（ｘ）＝$x^8+x^4+x^3+x^2+1$を表している。図２の左端のフリップフロップ（x^0で示される）に１、その他のフリップフロップに０を初期設定し、１クロック毎に出力されるデータ列を１６進数で表記すると、０１，０２，０４，０８，１０，２０，４０，８０，１Ｄ，３Ａ，．．．，８Ｅ，０１，．．．の２５５回（＝2^8-1回）で周期的なデータ列となる。この出力データ列に２５６回目を００として加えれば、可逆的な８ビットのデータ変換ができる。そのデータ変換を１６進数であらわすと、００は０１、０１は０２、０２は０４、０３は０８，．．．，ＦＥは８Ｅ、ＦＦは００となる。またデータ逆変換は、００はＦＦ、０１は００、０２は０１、０３は１９，．．．，ＦＥは５８、ＦＦはＡＦとなる。但し、これはデータ変換の一例にすぎず、可逆的なデータ変換ができれば、どのような回路であってもよい。エラー訂正回路を備えた装置であれば、このような可逆データ変換が誤り訂正回路に予め存在するので、誤り訂正回路をデータ変換回路として流用することも可能である。

【００１２】

図３は、部分的に隠蔽されたプログラムの実行形式の作成フローチャートである。

【００１３】

（３０１）隠蔽すべき制御手順をプログラミングし、隠蔽の対象となるプログラムソース３１１を作成する。

【００１４】

（３０２）作成されたプログラムソース３１１をコンパイルおよびリンクして、実行形式のバイナリデータ３１２を生成する。

【００１５】

（３０３）実行形式のバイナリデータ３１２に、上述したデータ逆変換を施して、逆変換済みのバイナリデータ３１３を生成する。

【００１６】

（３０４）逆変換済みのバイナリデータ３１３を、他のプログラムソースに組み入れやすいように、プログラムソース形式（例えばＣ言語のchar型の配列表記を内容として持つインクルードファイル形式）である、逆変換済みのバイナリデータを表現するデータ配列３１４に変換する。

【００１７】

（３０５）逆変換済みのバイナリデータを表現するデータ配列３１４と隠蔽対象でない他の制御手順とを結合し、全プログラムソース３１５を作成する。

【００１８】

（３０６）全プログラムソース３１５をコンパイルおよびリンクして、装置のプログラムメモリ４に格納される実行形式のバイナリデータ３１６を生成する。

【００１９】

上述したバイナリデータ３１６は、予めプログラムメモリ４に書込まれて出荷されることもあるし、最近のパーソナルコンピュータのマザーボードで見かけられるように、フラッシュメモリを用いたプログラムメモリを更新するために、インターネット経由でバイナリデータ３１６の最新バージョンが配布されることもある。バイナリデータ３１６は、例え逆アセンブルといった手法を用いても、隠蔽された制御手順を解析することはできない。

【００２０】

図４は、隠蔽されたプログラムの実行フローチャートである。図５で示した隠蔽されたプログラムの領域を示した図と合わせて説明する。

【００２１】

（４０１）図５Ａで示されるように、プログラムメモリ４に格納された隠蔽されたプログラム５０１を、ＤＲＡＭ５に複製し、複製プログラム５０２を作る。

【００２２】

（４０２）図５Ｂで示されるように、ＤＲＡＭ５上の複製プログラム５０２を、データ変換回路３を用いて、復元プログラム５０３に復元する。

【００２３】

（４０３）図５Ｂで示される復元プログラム５０３の中の関数（モジュールとも呼ぶ）を呼び出す。関数の呼び出しに関する詳細は後述する。

【００２４】

（４０４）呼び出した関数から戻ってきた後に、図５Ｃで示されるように、復元プログラム５０３が存在した領域５０４を、値０で埋めるなどして消去する。

【００２５】

ステップ（４０２）の復元処理を、全てソフトウェアで実行する場合、この箇所を解析されれば、隠蔽されたプログラムが解読される危険性がある。本発明の実施の形態では、装置１に固有のハードウェアであるデータ変換回路３を用いることで、隠蔽されたプログラムを解読から守ることができる。

【００２６】

次に、関数の呼び出し方法について説明する。図６は、隠蔽対象のプログラムの構造を示す図である。隠蔽対象のプログラムは、外部から呼び出される公開関数６１と６２と、内部から相対番地で呼び出される内部関数６３と６４と６５と、隠蔽対象のプログラムの先頭からみた公開関数６１と６２の相対番地を列挙した相対番地リスト６０から構成される。これらの番地の情報は、図５Ａの複製プログラム５０２の位置に依存しない情報であり、図３の対象プログラムソース３１１から得ることができる。

【００２７】

図７は、マイコン２から見たアドレス空間を示す図である。プログラムメモリ４とＤＲＡＭ５は、マイコン２から見ると、それぞれ独自の番地が割付けられた領域に配置される。逆変換されたプログラム（図７中のプログラムメモリのハン

チングされた領域）から複製され復元された復元プログラム（図７中のＤＲＡＭのハンチングされた領域）は、マイコン２が指定した所定の番地（図７中の複製した先頭番地）から配置される。従って、公開関数１のマイコンから見た絶対番地は、複製した先頭番地に公開関数１の相対番地を加算することによって求められる。この絶対番地を指定することで、公開関数１を呼び出すことができる。公開関数２についても同様である。

【００２８】

【発明の効果】

以上説明したように、本発明の実施の形態によれば、部分的に隠蔽された制御プログラムを作成でき、この隠蔽された制御プログラムを安全に復元して実行することができる。プログラムの復元アルゴリズムは、装置に組み込まれたハードウェアとで分担しているので、非常に高度なソフトウェア技術を有した人物であっても、制御プログラムだけを解析しても分からない。用いるハードウェアは簡単な回路でも、充分な解読に対する抵抗力を持つことができるので、隠蔽すべき処理を全てのハードウェアで実現したり、もしくは全てソフトウェアで実現するのに比較して、開発期間とコストと安全性の面で優れている。

【図面の簡単な説明】

【図１】

本発明の実施の形態における装置の構成の一例を示すブロック図

【図２】

データ変換回路の一例を示す回路図

【図３】

部分的に隠蔽されたプログラムの実行形式の作成フローチャート

【図４】

隠蔽されたプログラムの実行フローチャート

【図５Ａ】

プログラム複製処理におけるプログラム領域の配置図

【図５Ｂ】

プログラム変換処理におけるプログラム領域の配置図

【図５Ｃ】

プログラム消去処理におけるプログラム領域の配置図

【図６】

隠蔽対象のプログラムの構造図

【図７】

マイコンから見たアドレス空間図

【符号の説明】

１　装置

２　マイコン

３　データ変換回路

４　プログラムメモリ

５　ＤＲＡＭ

６　その他の回路

７　内部バス

６０　相対番地リスト

６１，６２　公開関数

６３，６４，６５　内部関数

３１１　対象プログラムソース

３１２　実行形式のバイナリデータ

３１３　逆変換済みのバイナリデータ

３１４　逆変換済みのバイナリデータを表現するデータ配列

３１５　全プログラムソース

３１６　プログラムメモリに格納される実行形式のバイナリデータ

５０１　隠蔽されたプログラム

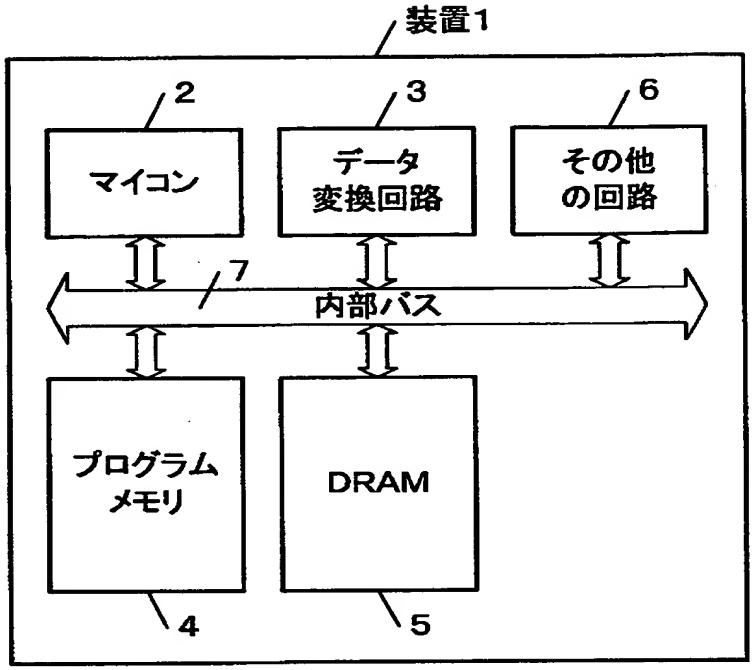
５０２　複製プログラム

５０３　復元プログラム

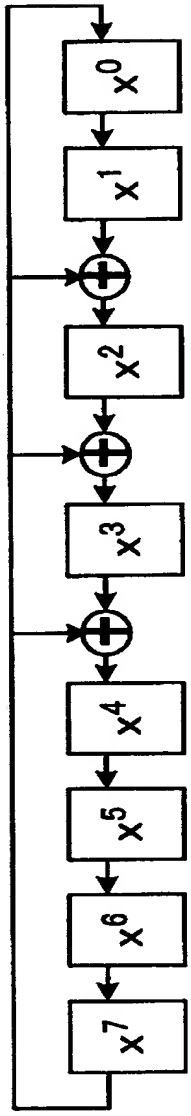
５０４　消去されたプログラム領域

【書類名】　　図面

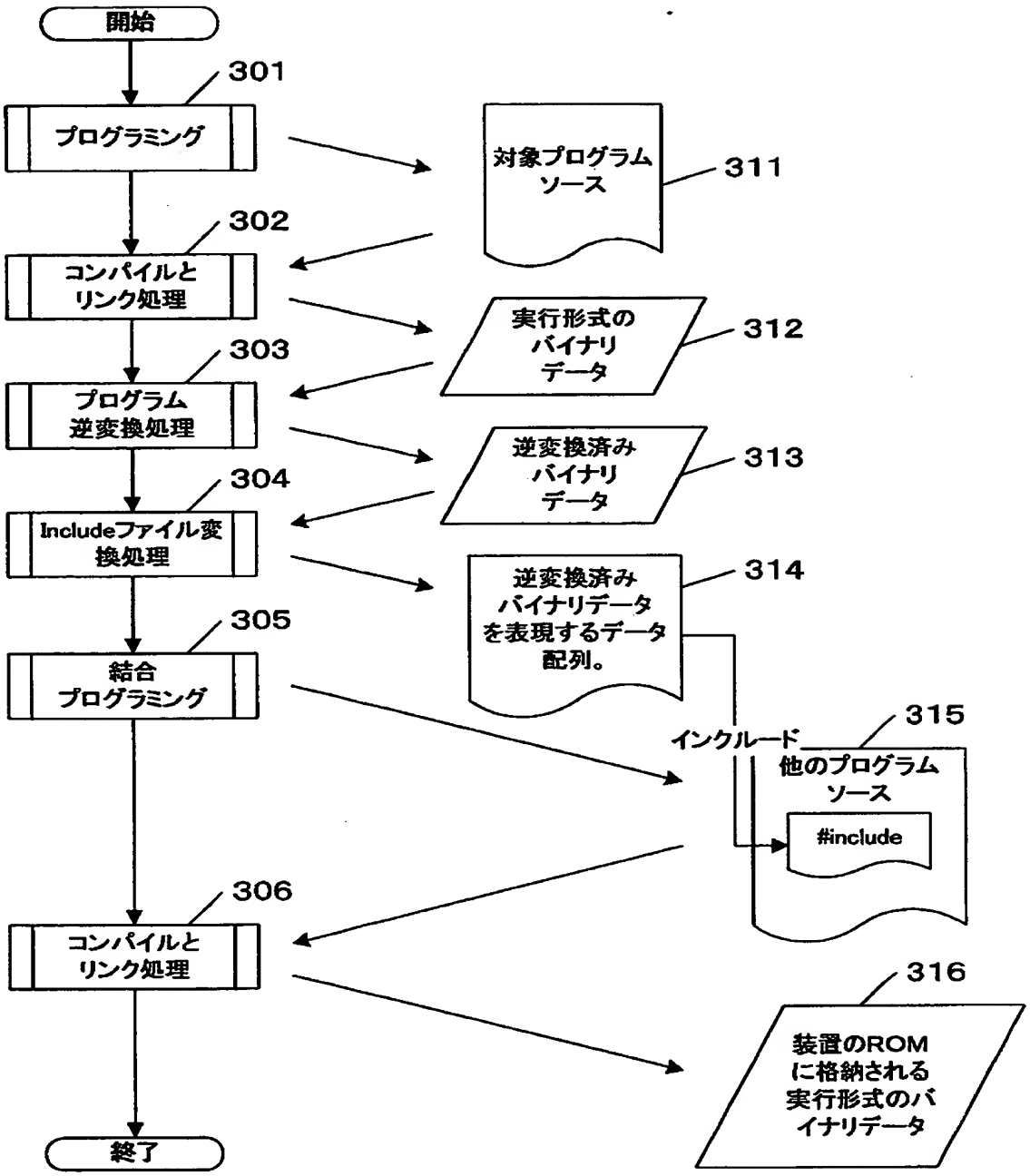
【図１】



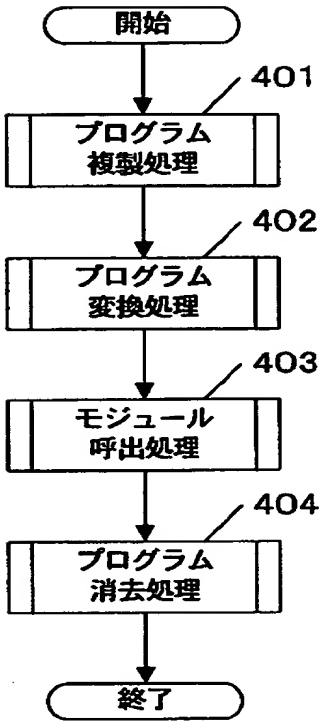
【図２】



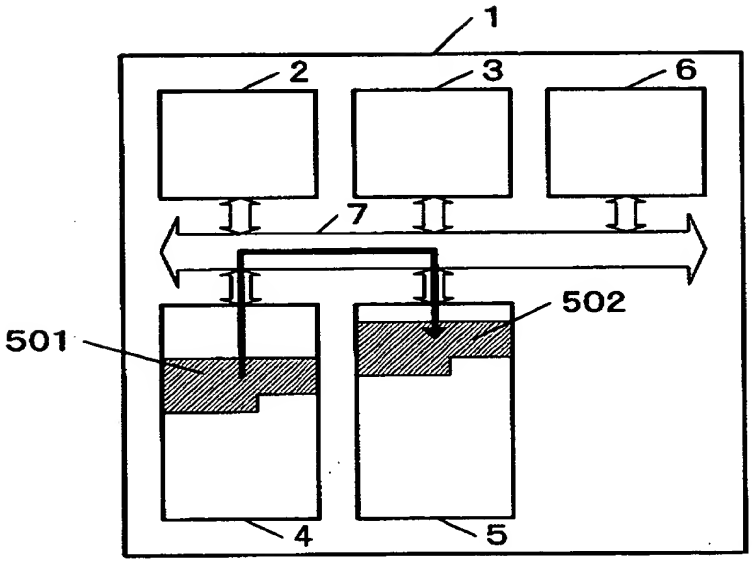
【図３】


開始
301
プログラミング
対象プログラム
ソース
311
302
コンパイルと
リンク処理
実行形式の
バイナリ
データ
312
303
プログラム
逆変換処理
逆変換済み
バイナリ
データ
313
304
Includeファイル変
換処理
逆変換済み
バイナリデータ
を表現するデータ
配列。
314
305
結合
プログラミング
インクルード
315
他のプログラム
ソース
#include
306
コンパイルと
リンク処理
316
装置のROM
に格納される
実行形式のバ
イナリデータ
終了

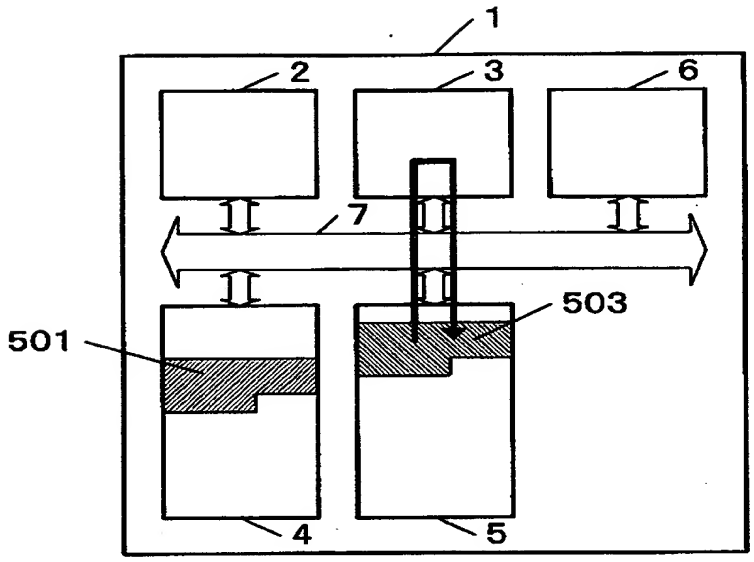
【図４】


開始
401
プログラム
複製処理
402
プログラム
変換処理
403
モジュール
呼出処理
404
プログラム
消去処理
終了

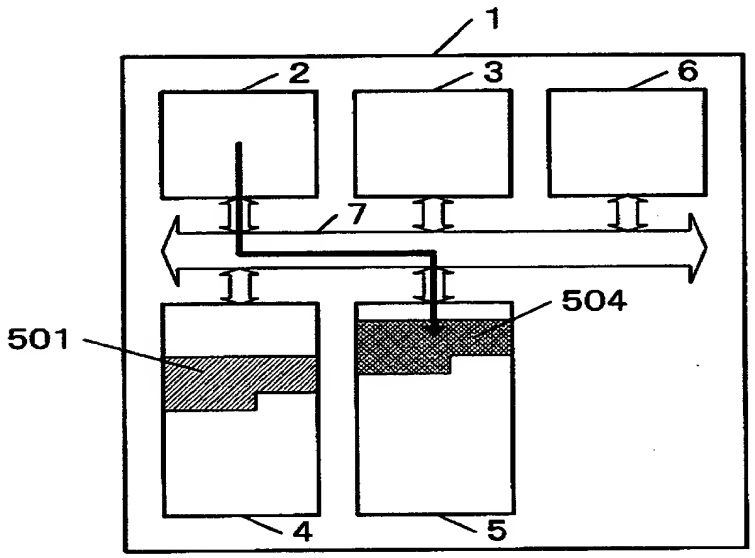
【図５Ａ】


1
2
3
6
7
501
502
4
5

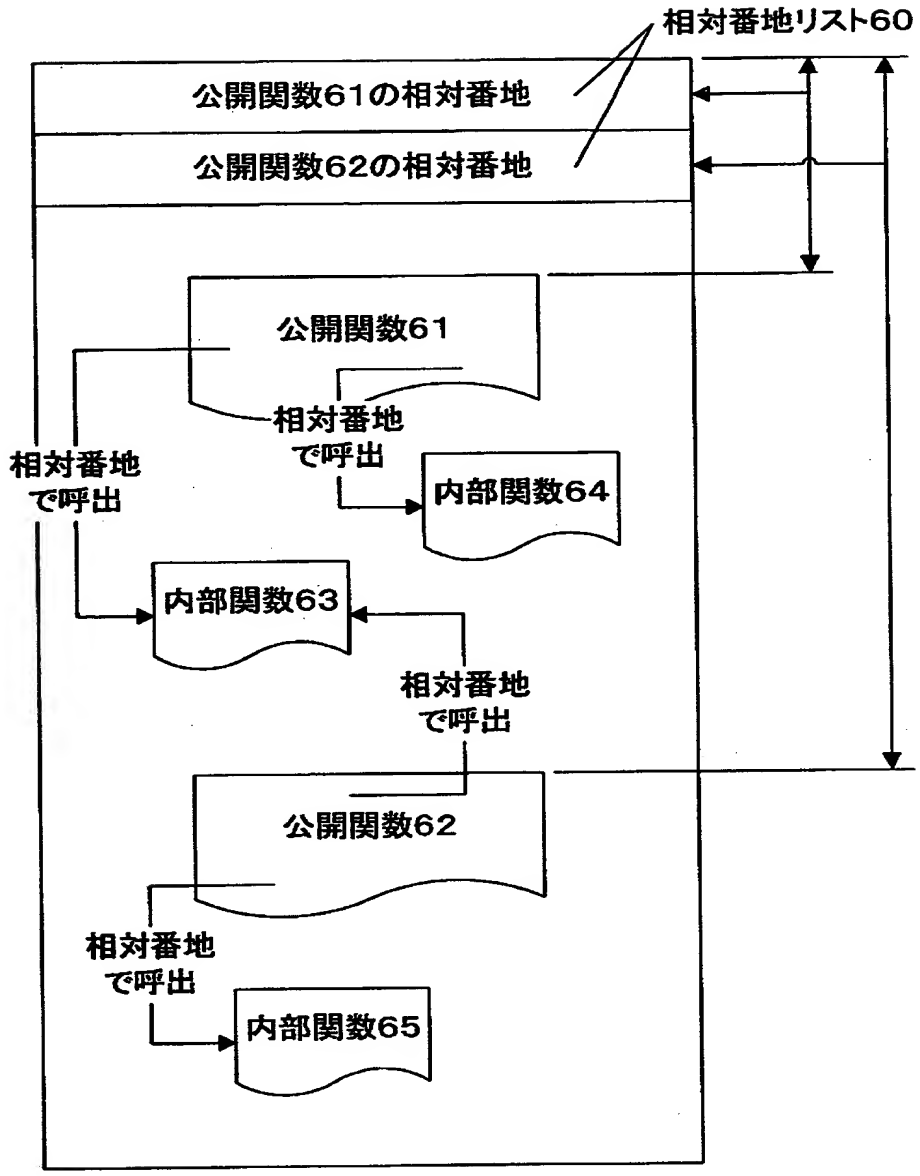
【図５Ｂ】



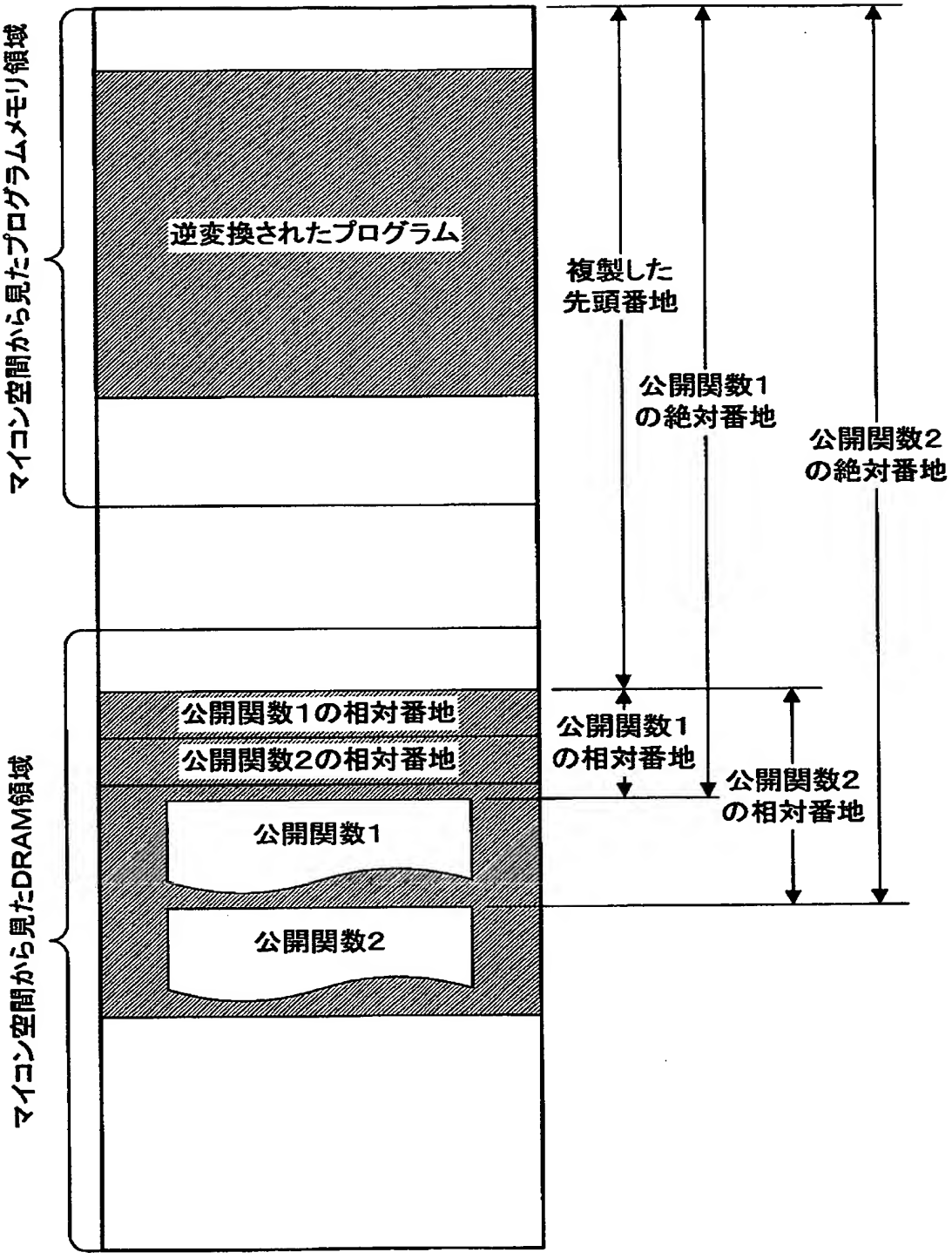
【図５Ｃ】



【図６】


相対番地リスト60
公開関数61の相対番地
公開関数62の相対番地
公開関数61
相対番地
で呼出
内部関数64
相対番地
で呼出
内部関数63
相対番地
で呼出
公開関数62
相対番地
で呼出
内部関数65

【図７】


マイコン空間から見たプログラムメモリ領域
逆変換されたプログラム
複製した
先頭番地
公開関数1
の絶対番地
公開関数2
の絶対番地
マイコン空間から見たDRAM領域
公開関数1の相対番地
公開関数2の相対番地
公開関数1
公開関数2
公開関数1
の相対番地
公開関数2
の相対番地

【書類名】　要約書

【要約】

【課題】　著作権保護機能などを装置に導入する場合、その機能自身を第三者による解読から守るために隠蔽する必要がある。ＬＳＩに機能を隠蔽する場合は、開発期間とコストがかかる。ソフトウェアに機能を隠蔽する場合は、隠蔽強度を持たせるのが困難である。

【解決手段】　装置に備わる可逆変換を行うデータ変換回路に着目し、隠蔽対象となる機能を実現する制御プログラムにデータ変換回路の逆変換を施してプログラムメモリに保存し、隠蔽対象の制御プログラムの復元処理をデータ変換回路で行う。従って、制御プログラムに自分自身の復元アルゴリズムが存在しないので、隠蔽強度を高めることができる。

【選択図】　図３

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社